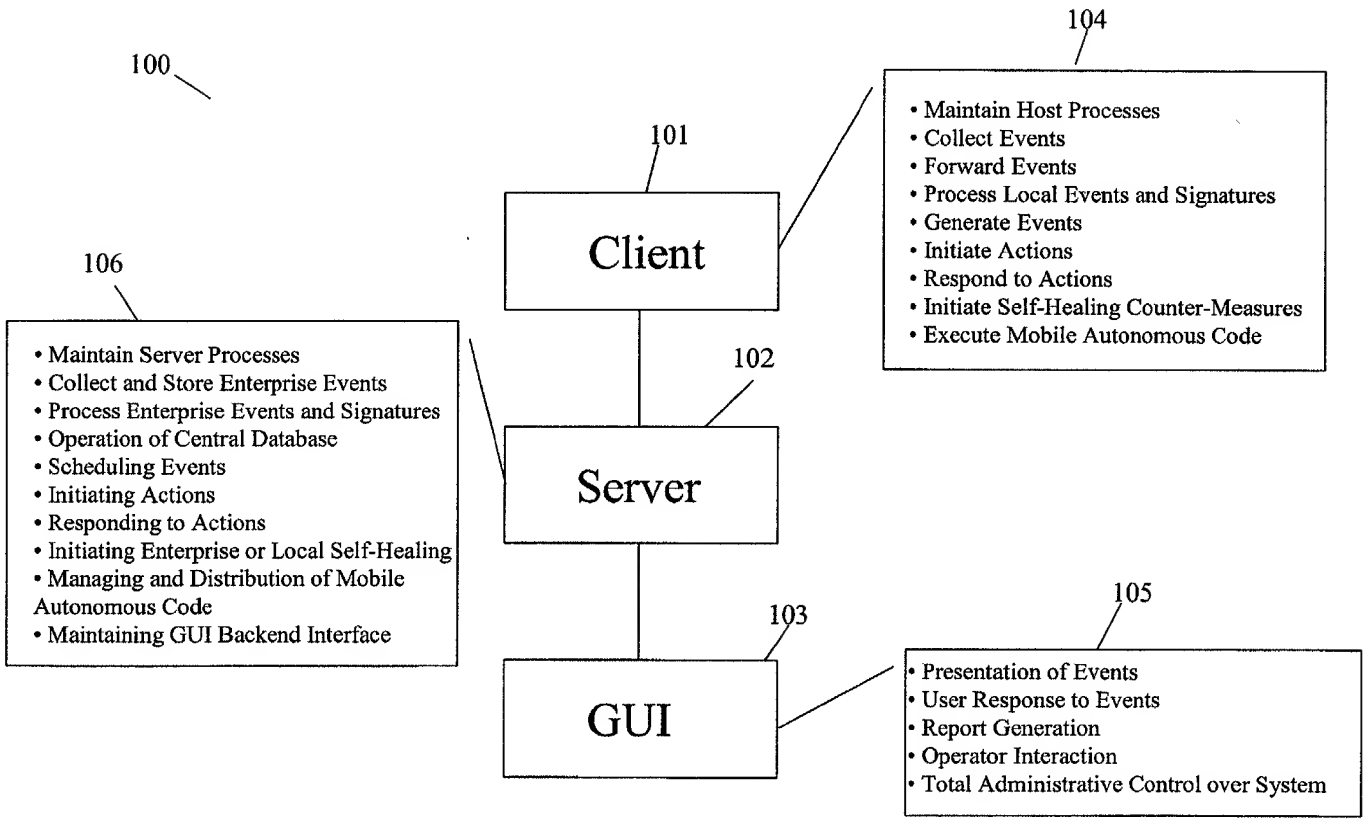

100
101
Client
104
• Maintain Host Processes
• Collect Events
• Forward Events
• Process Local Events and Signatures
• Generate Events
• Initiate Actions
• Respond to Actions
• Initiate Self-Healing Counter-Measures
• Execute Mobile Autonomous Code
106
• Maintain Server Processes
• Collect and Store Enterprise Events
• Process Enterprise Events and Signatures
• Operation of Central Database
• Scheduling Events
• Initiating Actions
• Responding to Actions
• Initiating Enterprise or Local Self-Healing
• Managing and Distribution of Mobile Autonomous Code
• Maintaining GUI Backend Interface
102
Server
103
GUI
105
• Presentation of Events
• User Response to Events
• Report Generation
• Operator Interaction
• Total Administrative Control over System

Fig. 1

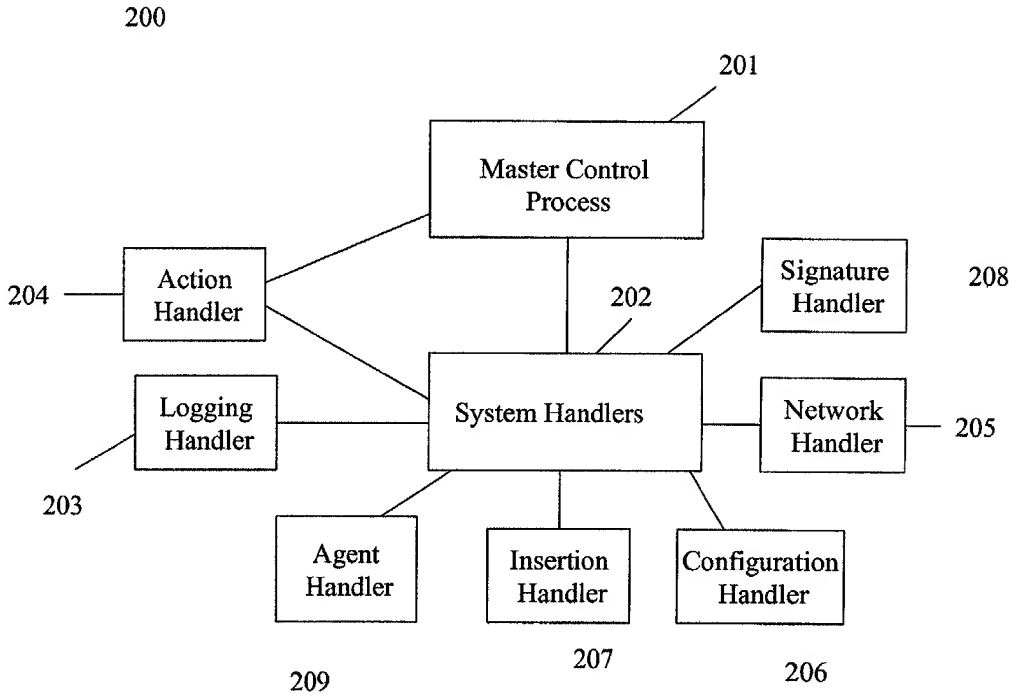

200
201
Master Control Process
204
Action Handler
202
Signature Handler
208
System Handlers
Logging Handler
Network Handler
205
203
Agent Handler
Insertion Handler
Configuration Handler
209
207
206

Fig. 2

20070129.0826

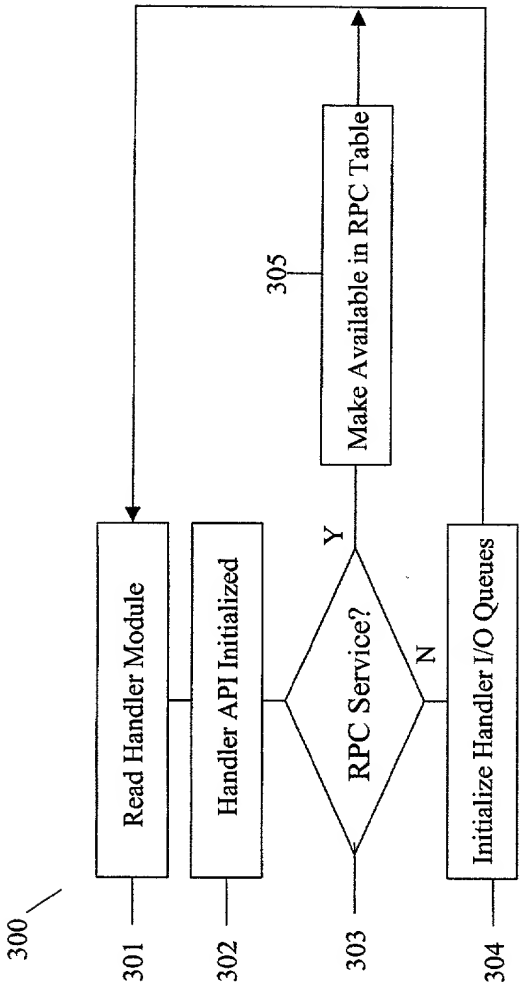


Fig. 3

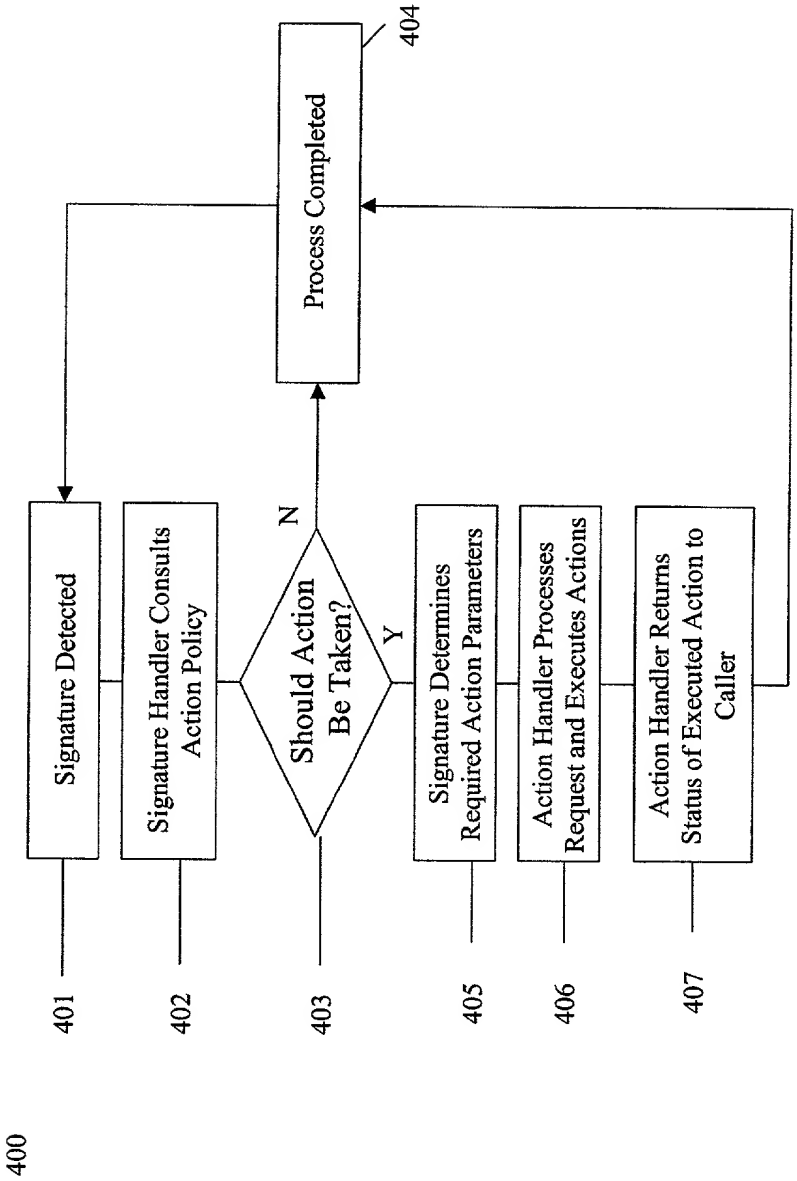

400
401
Signature Detected
402
Signature Handler Consults Action Policy
403
Should Action Be Taken?
N
Y
404
Process Completed
405
Signature Determines Required Action Parameters
406
Action Handler Processes Request and Executes Actions
407
Action Handler Returns Status of Executed Action to Caller

Fig. 4

Server
507
Client
506
Network Handler
501
Network Communication Encryption
505
Network Communication Compression
504
Network Authentication
503
Client/server Common Network
502
Access Control List
508

Fig. 5

MCP
601
Insertion Library
602
Named Pipe
605
Network Socket
604
File Descriptor
603
External Program Event N+1
607
External Program Event N
606
600

Fig. 6

APP_ID=09683507

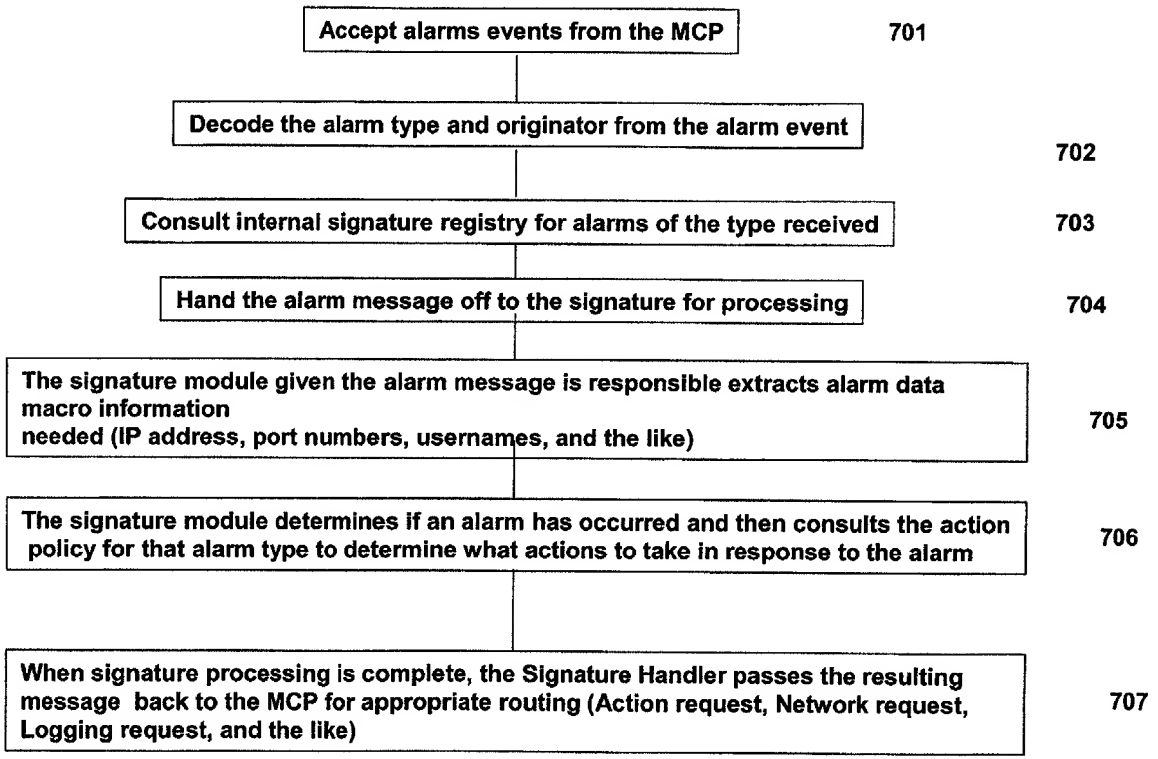


Fig. 7

APP_ID=09683507

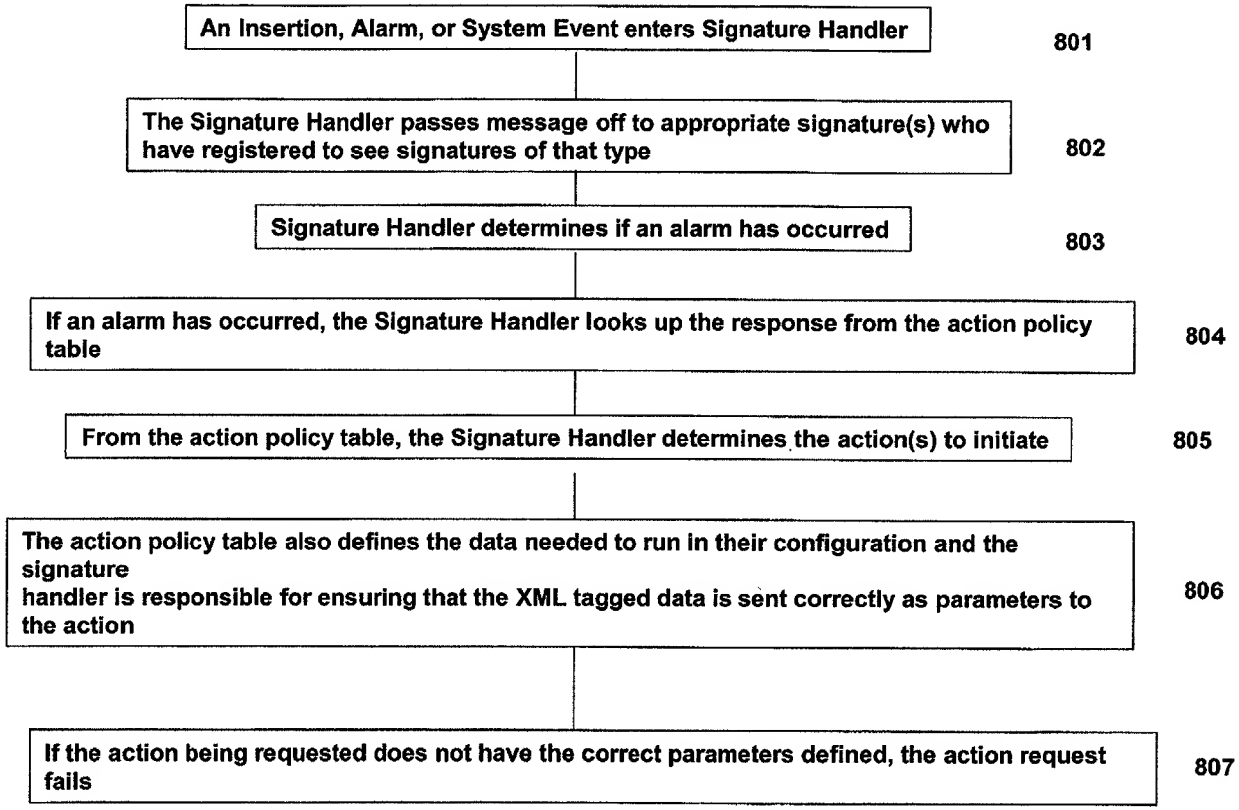


Fig. 8

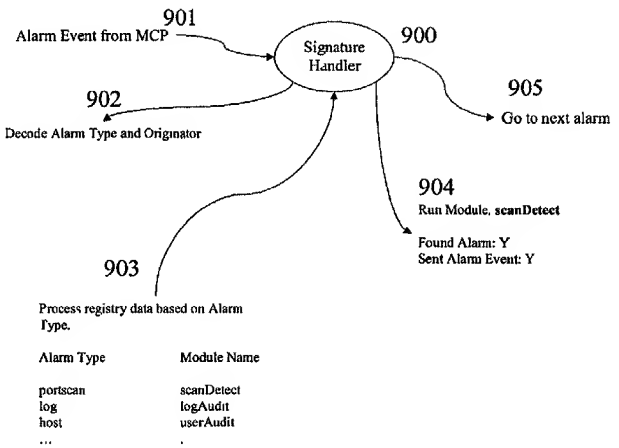

901
Alarm Event from MCP
Signature Handler
900
905
Go to next alarm
902
Decode Alarm Type and Originator
904
Run Module, scanDetect
Found Alarm: Y
Sent Alarm Event: Y
903
Process registry data based on Alarm Type.
Alarm Type
Module Name
portscan
scanDetect
log
logAudit
host
userAudit
...

Fig. 9

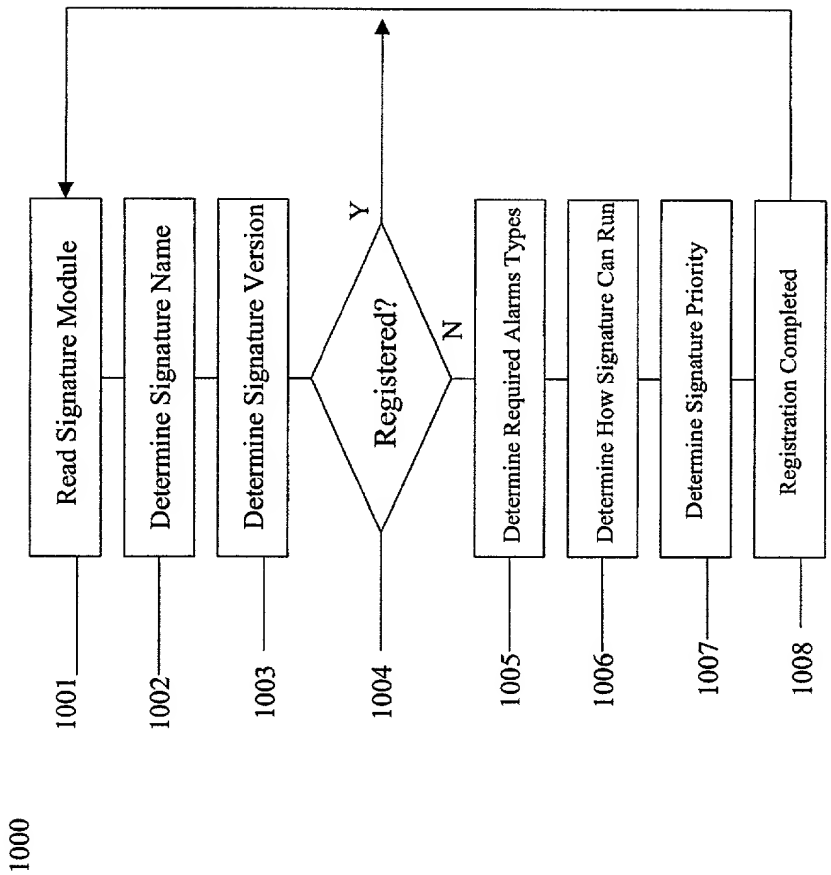

1000
Read Signature Module
Determine Signature Name
Determine Signature Version
Registered?
Y
N
Determine Required Alarms Types
Determine How Signature Can Run
Determine Signature Priority
Registration Completed
1001
1002
1003
1004
1005
1006
1007
1008

Fig. 10

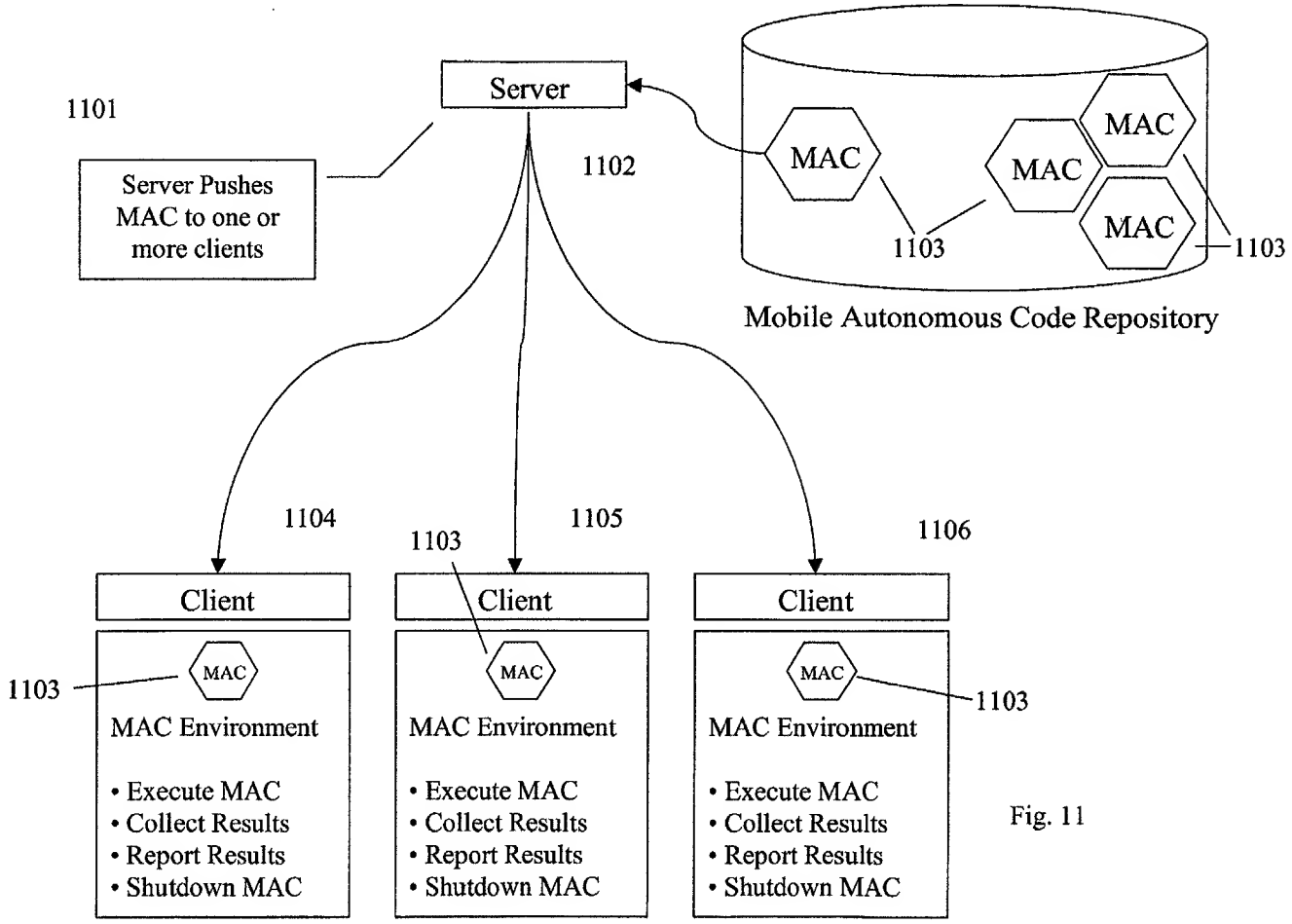
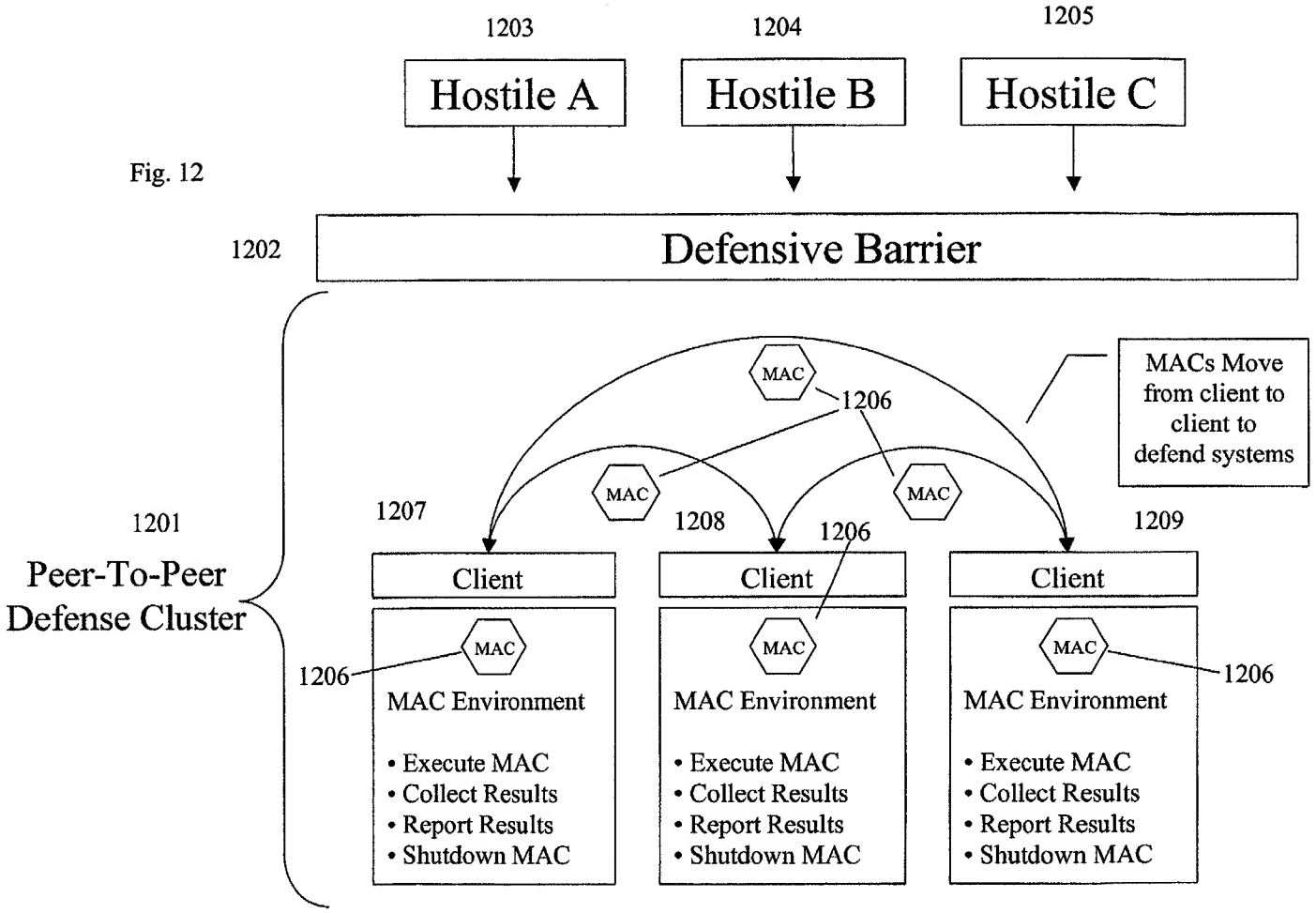

Server
1101
Server Pushes MAC to one or more clients
1102
MAC
MAC
MAC
MAC
1103
1103
Mobile Autonomous Code Repository
1104
1103
1105
1106
Client
Client
Client
1103
MAC
MAC
MAC
1103
MAC Environment
• Execute MAC
• Collect Results
• Report Results
• Shutdown MAC
MAC Environment
• Execute MAC
• Collect Results
• Report Results
• Shutdown MAC
MAC Environment
• Execute MAC
• Collect Results
• Report Results
• Shutdown MAC

Fig. 11

Fig. 12


1203
1204
1205
Hostile A
Hostile B
Hostile C
1202
Defensive Barrier
MAC
1206
MACs Move from client to client to defend systems
MAC
MAC
1207
1208
1206
1209
1201
Peer-To-Peer Defense Cluster
Client
Client
Client
MAC
1206
MAC
MAC
1206
MAC Environment
• Execute MAC
• Collect Results
• Report Results
• Shutdown MAC
MAC Environment
• Execute MAC
• Collect Results
• Report Results
• Shutdown MAC
MAC Environment
• Execute MAC
• Collect Results
• Report Results
• Shutdown MAC

APP_ID=09683507

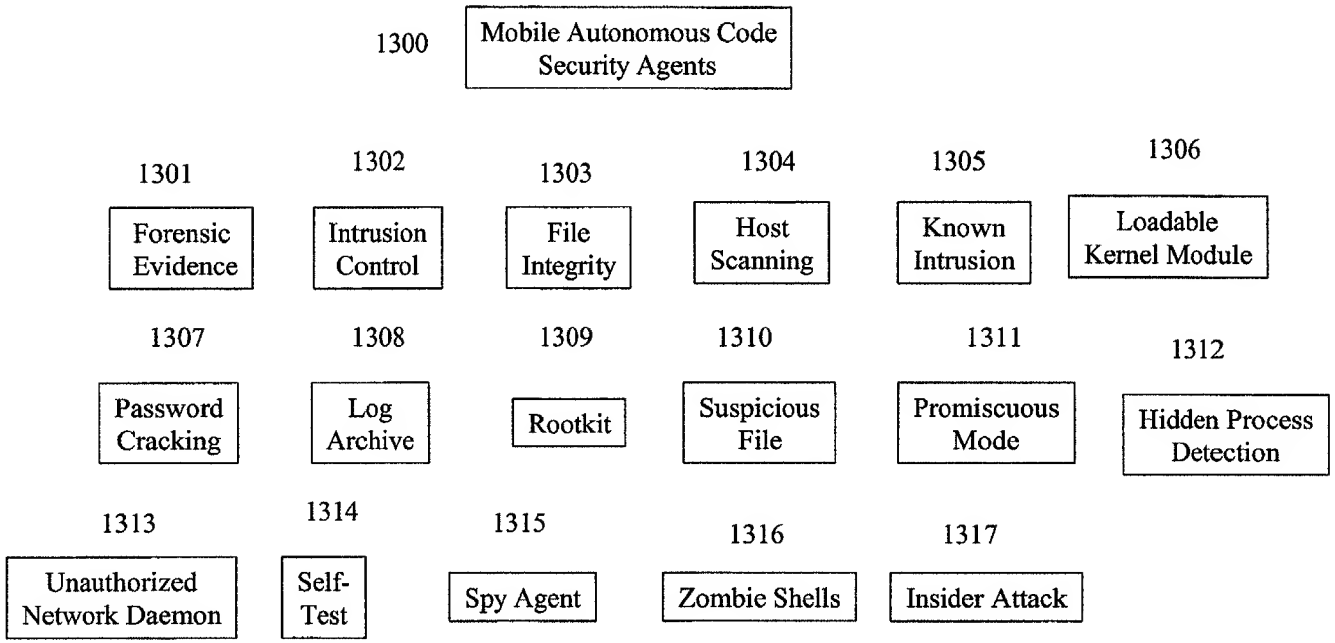


Fig. 13

APP_ID=09683507

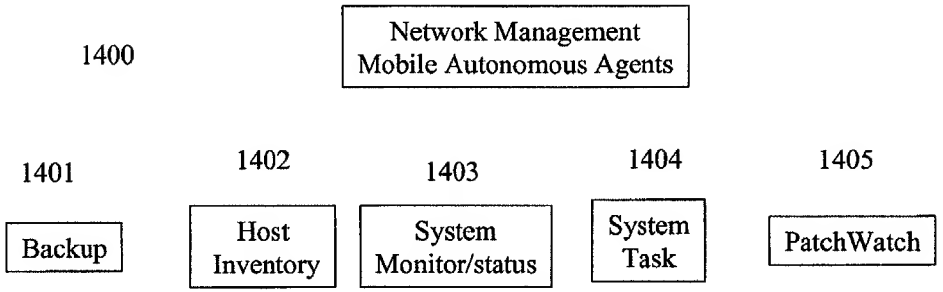


Fig. 14